NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

A. The website is exempted from SSL inspection.

B. The EICAR test file exceeds the protocol options oversize limit.

C. The selected SSL inspection profile has certificate inspection enabled.

D. The browser does not trust the FortiGate self-signed CA certificate.

Correct Answer: AC

SSL Inspection Profile, on the Inspection method there are 2 options to choose from, SSL Certificate Inspection or Full SSL Inspection. FG SEC 7.2 Studi Guide: Full SSL Inspection level is the only choice that allows antivirus to be effective.

QUESTION 2

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH

B. HTTPS

C. FTM

D. FortiTelemetry

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios

QUESTION 3

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.

B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

D. The IP version of the sources and destinations in a policy must match.

E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Correct Answer: BDE

QUESTION 4

An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

A. ZTNA IP/MAC filtering mode

B. ZTNA access proxy

C. SSL VPN

D. L2TP

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."

This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials.

ZTNA access proxy uses a secure tunnel between the user\\'s device and the FortiGate, and authenticates the user based on device identity and context.

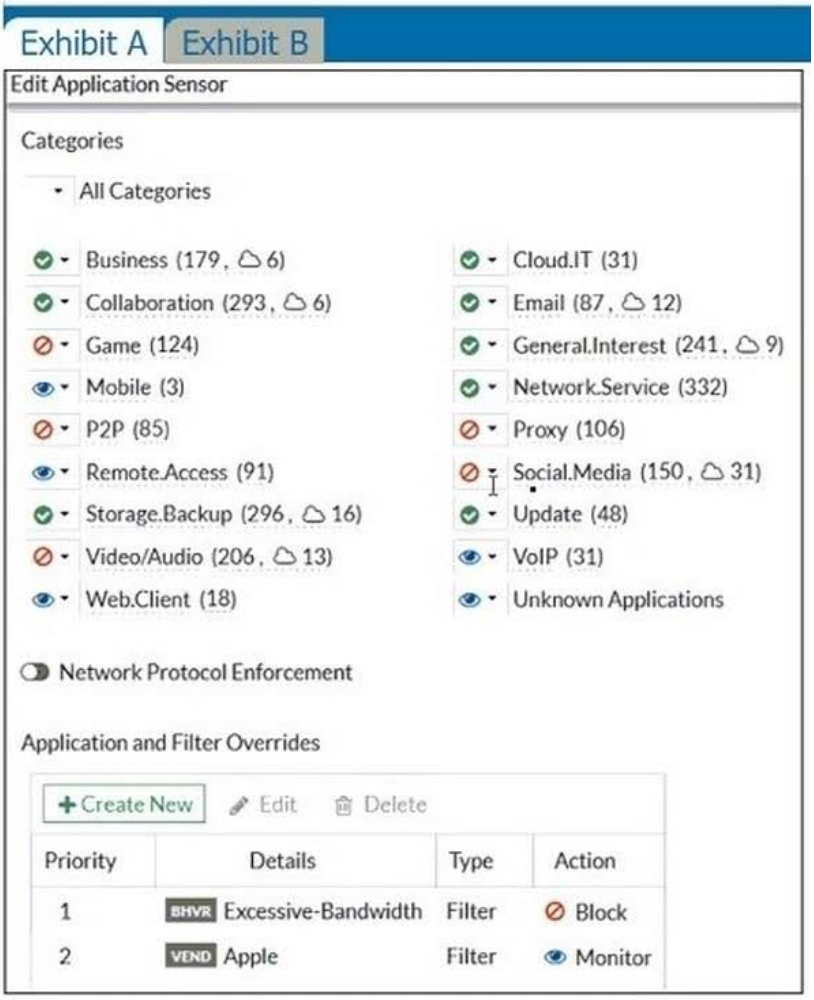
The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile.

This simplifies remote access and enhances security by reducing the attack surface12

QUESTION 5

Refer to the exhibits.

Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive- Bandwidth and Apple filter details.



Edit Application Sensor

Categories

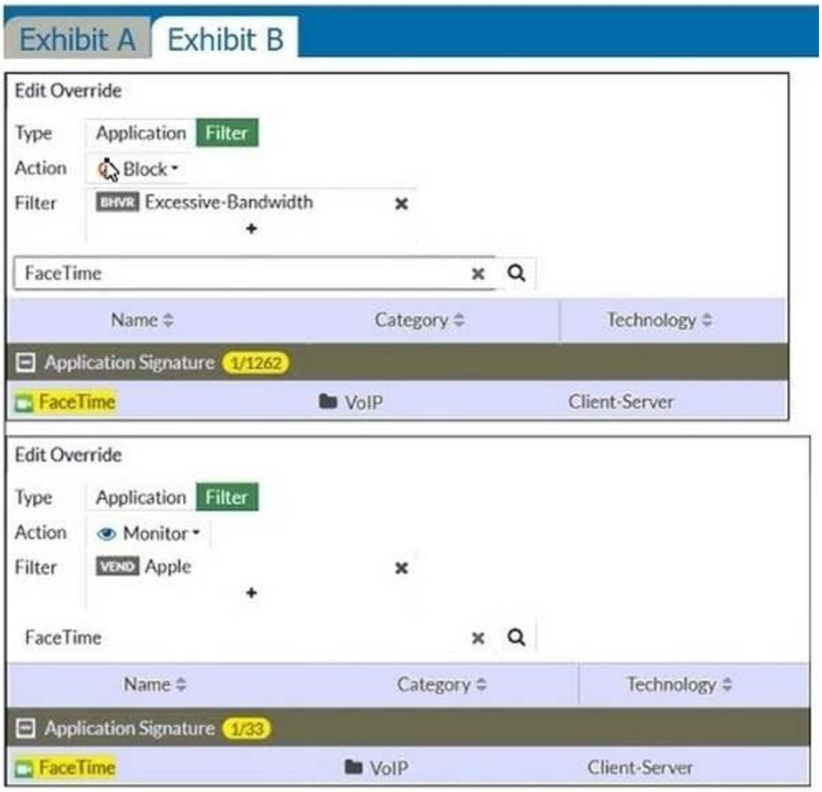
All Categories

- ✓ Business (179, ☁ 6)
- ✓ Collaboration (293, ☁ 6)
- ⊘ Game (124)
- 👁 Mobile (3)
- ⊘ P2P (85)
- 👁 Remote.Access (91)
- ✓ Storage.Backup (296, ☁ 16)
- ⊘ Video/Audio (206, ☁ 13)
- 👁 Web.Client (18)
- ✓ Cloud.IT (31)
- ✓ Email (87, ☁ 12)
- ✓ General.Interest (241, ☁ 9)
- ✓ Network.Service (332)
- ⊘ Proxy (106)
- ⊘ Social.Media (150, ☁ 31)
- ✓ Update (48)
- 👁 VoIP (31)
- 👁 Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Apple	Filter	👁 Monitor



Edit Override

Type: Application **Filter**
Action: Block
Filter: BHVR Excessive-Bandwidth

FaceTime

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Edit Override

Type: Application **Filter**
Action: 👁 Monitor
Filter: VEND Apple

FaceTime

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

A. Apple FaceTime will be allowed, based on the Categories configuration.

B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.

C. Apple FaceTime will be allowed, based on the Apple filter configuration.

D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Correct Answer: B

FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you\\'ve configured for applications in your selected categories."